Which feature does Cisco TrustSec use to provide scalable, secure communication throughout a network?

- security group tag number assigned to each port on a network
- security group tag ACL assigned to each port on a switch
- security group tag ACL assigned to each router on a network
- security group tag number assigned to each user on a switch

An engineer is configuring local web authentication on a WLAN. The engineer chooses the Authentication radio button under the Layer 3 Security options for Web Policy. Which device presents the web authentication for the WLAN?

- ISE server
- anchor WLC
- RADIUS server
- local WLC

An engineer configures GigabitEthernet 0/1 for VRRP group 115. The router must assume the primary role when it has the highest priority in the group. Which command set is required to complete this task?

```
interface GigabitEthernet0/1
ip address 10.10.10.2 255.255.255.0
vrrp 115 ip 10.10.10.1
vrrp 115 authentication 406457923
```

- Router(config-if)# **vrrp 115 track 1 decrement 10**
  Router(config-if)# **vrrp 115 preempt**
- Router(config-if)# **standby 115 priority 100**
  Router(config-if)# **standby 115 preempt**
- Router(config-if)# **vrrp 115 track 1 decrement 100**
  Router(config-if)# **vrrp 115 preempt**
- Router(config-if)# **vrrp 115 priority 100**

R1	R2

key chain cisco123
 key 1
  key-string Cisco123!
	key chain cisco123
	 key 1
	  key-string cisco123!

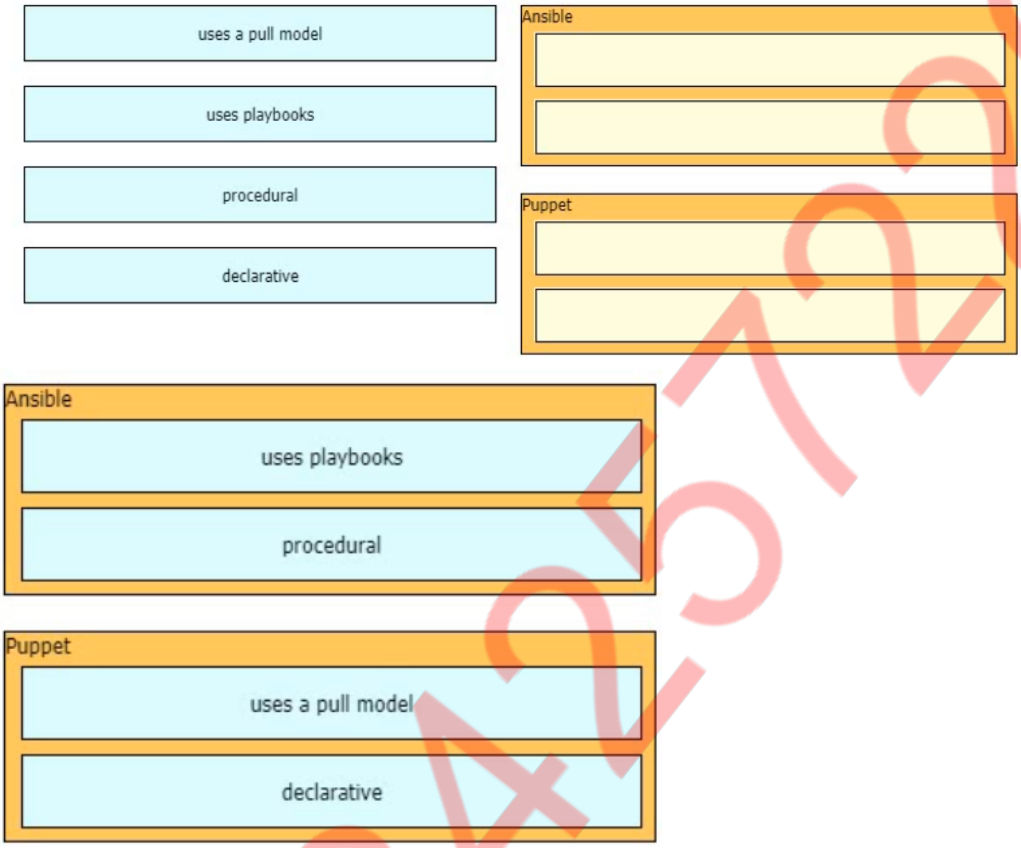
Ethernet0/0 - Group 10
  State is Active
  8 state changes, last state change 00:02:49
  Virtual IP address is 192.168.0.1
  Active virtual MAC address is 0000.0c07.ac0a
  Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 5 sec, hold time 15 sec
  Next hello sent in 2.880 secs
  Authentication MD5, key-chain "cisco123"
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 255 (configured 255)
  Group name is "workstation-group" (cfgd)
	Ethernet0/0 - Group 10
	  State is Active
	  17 state changes, last state change 00:02:17
	  Virtual IP address is 192.168.0.1
	  Active virtual MAC address is 0000.0c07.ac0a
	  Local virtual MAC address is 0000.0c07.ac0a (v1 default)
	  Hello time 10 sec, hold time 30 sec
	  Next hello sent in 6.720 secs
	  Authentication MD5, key-chain "cisco123"
	  Preemption disabled
	  Active router is local
	  Standby router is unknown
	  Priority 200 (configured 200)
	  Group name is "workstation-group" (cfgd)

Refer to the exhibit. An engineer is installing a new pair of routers in a redundant configuration. When checking on the standby status of each router, the engineer notices that the routers are not functioning as expected. Which action will resolve the configuration error?

- configure matching hold and delay timers
- configure matching key-strings
- configure matching priority values
- configure unique virtual IP addresses

+923034257226

Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

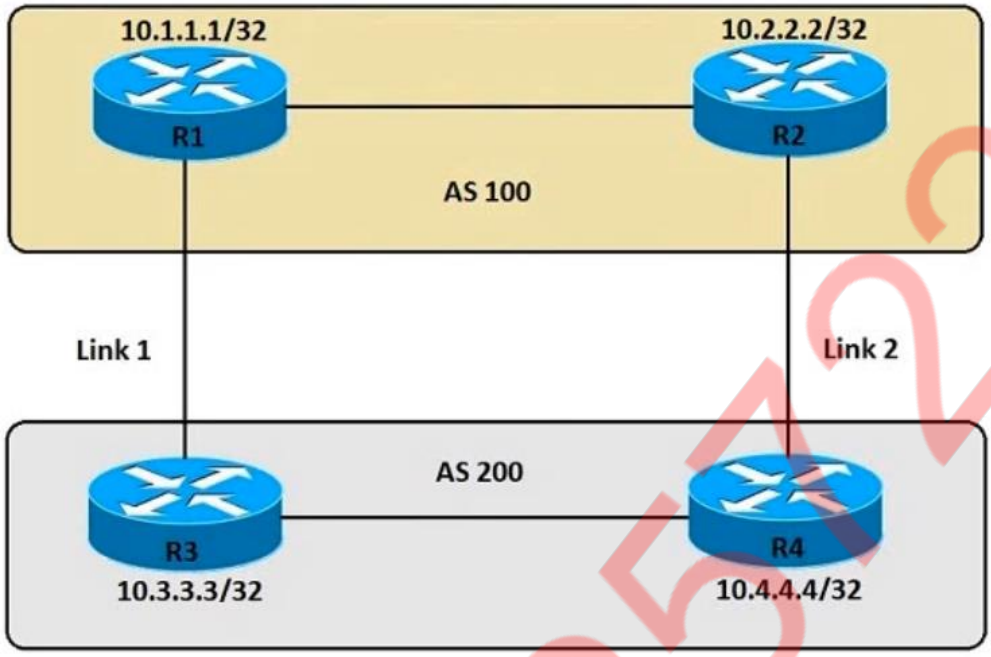



```
Extended IP access list EGRESS
10 permit ip 10.0.0.0 0.0.0.255 any
!
<Output Omitted>
!
interface GigabitEthernet0/0
 ip address 209.165.200.225 255.255.255.0
 ip access-group EGRESS out
 duplex auto
 speed auto
 media-type rj45
!
```

Refer to the exhibit. An engineer must block all traffic from a router to its directly connected subnet 209.165.200.0/24. The engineer applies access control list EGRESS in the outbound direction on the GigabitEthernet0/0 interface of the router. However, the router can still ping hosts on the 209.165.200.0/24 subnet. What explains this behavior?

- The access control list must contain an explicit deny to block traffic from the router.
- After an access control list is applied to an interface, that interface must be shut and no shut for the access control list to take effect.
- Access control lists that are applied outbound to a router interface do not affect traffic that is sourced from the router.
- Only standard access control lists can block traffic from a source IP address.

+923334257268



Refer to the exhibit. An engineer must ensure that all traffic entering AS 200 from AS 100 chooses Link 2 as an entry point. Assume that all BGP neighbor relationships have been formed and that the attributes have not been changed on any of the routers. Which configuration accomplishes this task?

- R3(config)#**route-map PREPEND permit 10**
  R3(config-route-map)#**set as-path prepend 200 200 200**

  R3(config)#**router bgp 200**
  R3(config-router)#**neighbor 10.1.1.1 route-map PREPEND out**
- R3(config)#**route-map PREPEND permit 10**
  R3(config-route-map)#**set as-path prepend 100 100 100**

  R3(config)#**router bgp 200**
  R3(config-router)#**neighbor 10.1.1.1 route-map PREPEND in**
- R4(config)#**route-map PREPEND permit 10**
  R4(config-route-map)#**set as-path prepend 200 200 200**

  R4(config)#**router bgp 200**
  R4(config-router)#**neighbor 10.2.2.2 route-map PREPEND out**
- R4(config)#**route-map PREPEND permit 10**
  R4(config-route-map)#**set as-path prepend 100 100 100**

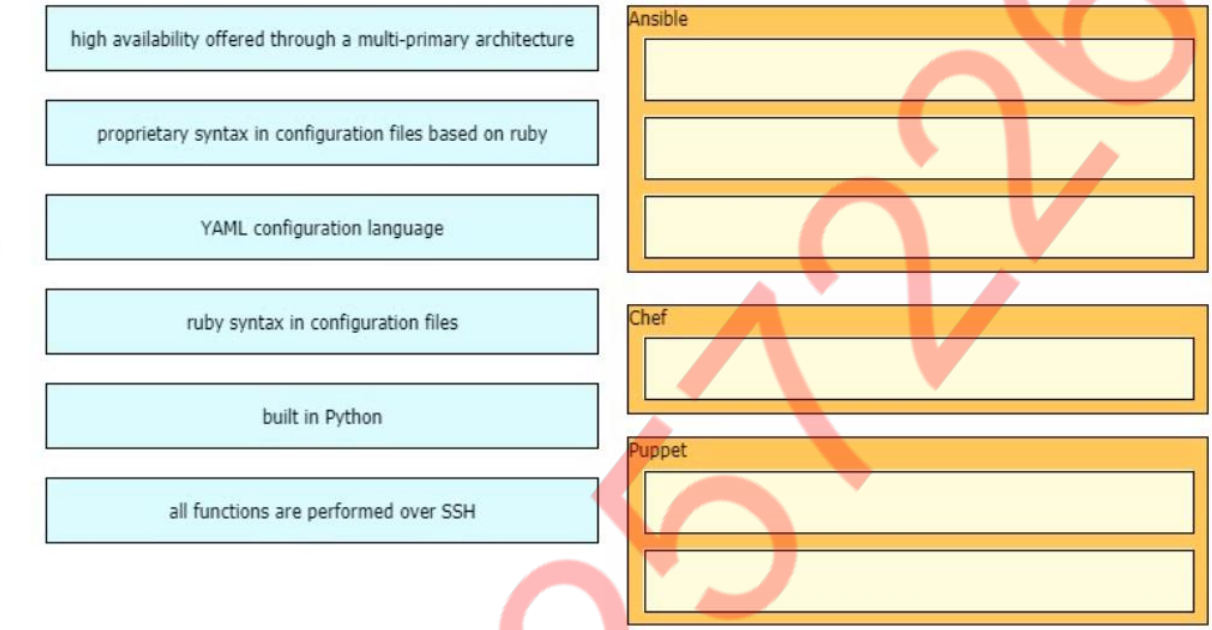
  R4(config)#**router bgp 200**
  R4(config-router)#**neighbor 10.2.2.2 route-map PREPEND in**

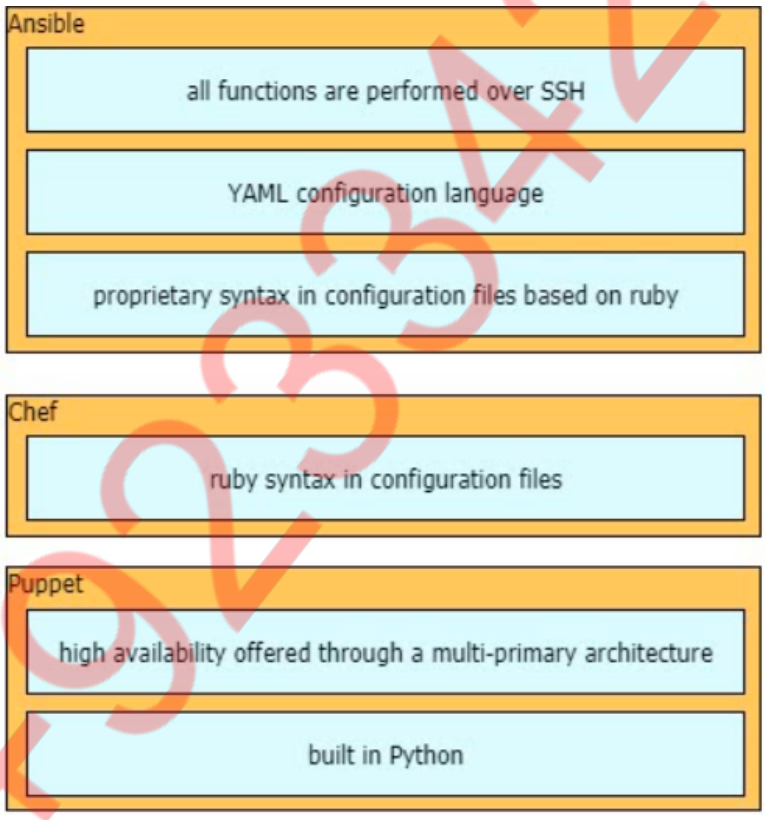
Which two operations are valid for RESTCONF? (Choose two.)

- [ ] PULL
- [x] PATCH
- [ ] REMOVE
- [x] HEAD
- [ ] PUSH
- [ ] ADD

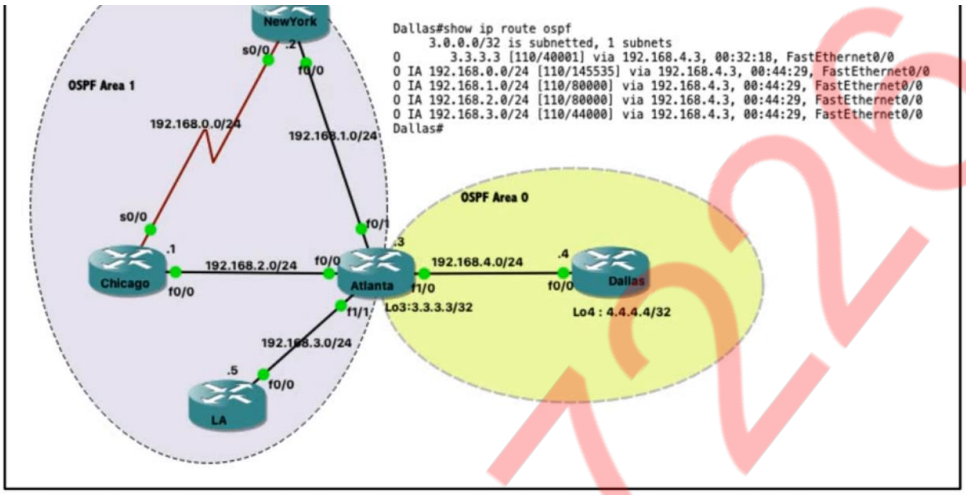
+923034252268

Drag and drop the automation characteristics from the left to the corresponding tools on the right.





x923342517268



Refer to the exhibit. When applied to the Atlanta router, which command reduces type 3 LSA flooding into the backbone area and summarizes the inter-area routes on the Dallas router?

- Atlanta(config-router)#**area 0 range 192.168.0.0 255.255.248.0**
- Atlanta(config-router)#**area 1 range 192.168.0.0 255.255.252.0**
- Atlanta(config-router)#**area 0 range 192.168.0.0 255.255.252.0**
- Atlanta(config-router)#**area 1 range 192.168.0.0 255.255.248.0**

An engineer must protect their company against ransomware attacks. Which solution allows the engineer to block the execution stage and prevent file encryption?

- Use Cisco Firepower and block traffic to TOR networks.
- Use Cisco Firepower with Intrusion Policy and snort rules blocking SMB exploitation.
- Use Cisco AMP deployment with the Malicious Activity Protection engine enabled.
- Use Cisco AMP deployment with the Exploit Prevention engine enabled.

When using TLS for syslog, which configuration allows for secure and reliable transportation of messages to its default port?

- **logging host 10.2.3.4 vrf mgmt transport tcp port 514**
- **logging host 10.2.3.4 vrf mgmt transport tcp port 6514**
- **logging host 10.2.3.4 vrf mgmt transport udp port 6514**
- **logging host 10.2.3.4 vrf mgmt transport udp port 514**

+923342517268

Which exhibit displays a valid JSON file?

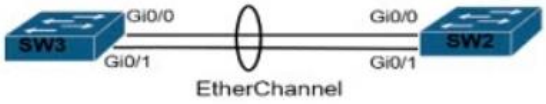
```
{
    "hostname": "edge_router_1",
    "interfaces": {
        "GigabitEthernet1/1",
        "GigabitEthernet1/2",
        "GigabitEthernet1/3",
    },
}
```

```
{
    "hostname": "edge_router_1"
    "interfaces": {
        "GigabitEthernet1/1"
        "GigabitEthernet1/2"
        "GigabitEthernet1/3"
    }
}
```

```
{
    "hostname": "edge_router_1"
    "interfaces": [
        "GigabitEthernet1/1"
        "GigabitEthernet1/2"
        "GigabitEthernet1/3"
    ]
}
```

```
{
    "hostname": "edge_router_1",
    "interfaces": [
        "GigabitEthernet1/1",
        "GigabitEthernet1/2",
        "GigabitEthernet1/3"
    ]
}
```

+923425722268




```
SW2# show ip interface brief | include Port
Port-channel1 unassigned YES unset down down
SW2# show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+-------------+-----------+--------------
-------
1 Pol(S D ) PAgP Gi0/0(I) Gi0/1(I)
```

```
SW3# show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+-------------+-----------+--------------
-------
1 Pol(S D ) LACP Gi0/0(I) Gi0/1(I)
```

Refer to the exhibit. Which action resolves the EtherChannel issue between SW2 and SW3?

- Configure **switchport mode trunk** on SW2.
- Configure **channel-group 1 mode active** on both interfaces.
- Configure **channel-group 5 mode desirable** on both interfaces.
- Configure **switchport nonegotiate** on SW3.

+923342572268

```
R1#  sh  run | begin line con
line con o
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux o
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 password 7 045802150C2E
 login
line vty 5 15
 password 7 045802150C2E
 login
!
end

R1#  sh  run  |  include aaa | enable
no aaa new-model
R1#
```

Refer to the exhibit. Which privilege level is assigned to VTY users?

- 1

An engineer must protect their company against ransomware attacks. Which solution allows the engineer to block the execution stage and prevent file encryption?

- Use Cisco Firepower and block traffic to TOR networks.
- Use Cisco Firepower with Intrusion Policy and snort rules blocking SMB exploitation.
- Use Cisco AMP deployment with the Malicious Activity Protection engine enabled.
- Use Cisco AMP deployment with the Exploit Prevention engine enabled.

If the noise floor is -90 dBm and the wireless client is receiving a signal of -75 dBm, what is the SNR?

- 15
- 1.2
- -165
- .83

+923342572268

How is MSDP used to interconnect multiple PIM-SM domains?

- [x] MSDP depends on BGP or multiprotocol BGP for interdomain operation.
- [ ] MSDP messages are used to advertise active sources in a domain.
- [ ] MSDP SA request messages are used to request a list of active sources for a specific group.
- [ ] MSDP allows a rendezvous point to dynamically discover active sources outside of its domain.

What is the difference between the MAC address table and TCAM?

- [ ] Router prefix lookups happen in TCAM. MAC address table lookups happen in CAM.
- [ ] TCAM is used to make L2 forwarding decisions. CAM is used to build routing tables.
- [x] The MAC address table is contained in TCAM. ACL and QoS information is stored in CAM.
- [ ] The MAC address table supports partial matches. TCAM requires an exact match.

In Cisco SD-WAN, which protocol is used to measure link quality?

- [ ] IPsec
- [ ] OMP
- [ ] RSVP
- [x] BFD

+923342572268

```
SwitchC#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally      : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Transparent
VTP Domain Name                 : cisco.com
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xE5 0x28 0x5D 0x3E 0x2F 0xE5 0xAD 0x2B
Configuration last modified by 0.0.0.0 at 1-10-19 09:01:38

SwitchC#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Po1
110  Finance                          active
210  HR                               active    Fa0/1
310  Sales                            active    Fa0/2
[...output omitted...]

SwitchC#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig1/1      on           802.1q         trunking      1
Gig1/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig1/1      1-1005
Gig1/2      1-1005

Port        Vlans allowed and active in management domain
Gig1/1      1,110,210,310
Gig1/2      1,110,210,310

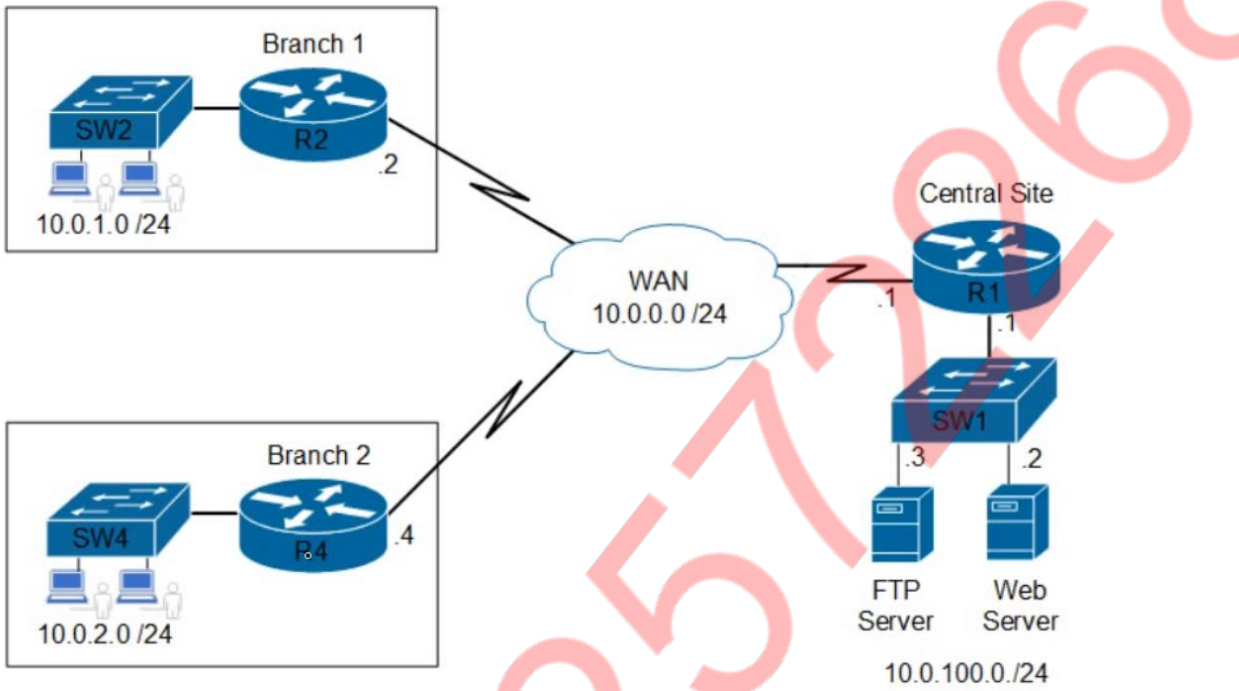
Port        Vlans in spanning tree forwarding state and not pruned
Gig1/1      1,110,210,310
Gig1/2      1,110,210,310

SwitchC#show run interface port-channel 1
interface Port-channel 1
 description Uplink_to_Core
 switchport mode trunk
```

Refer to the exhibit. SwitchC connects HR and Sales to the Core switch. However, business needs require that no traffic from the Finance VLAN traverse this switch. Which command meets this requirement?

- SwitchC(config)#**vtp pruning**
- SwitchC(config)#**interface port-channel 1**
  SwitchC(config-if)#**switchport trunk allowed vlan add 210,310**
- SwitchC(config)#**interface port-channel 1**
  SwitchC(config-if)#**switchport trunk allowed vlan remove 110**
- SwitchC(config)#**vtp pruning vlan 110**

+923342572268



Refer to the exhibit. A network engineer must monitor the response time from the branch offices to the central site. Which command set configures and activates the IPSLA feature in the R4 route

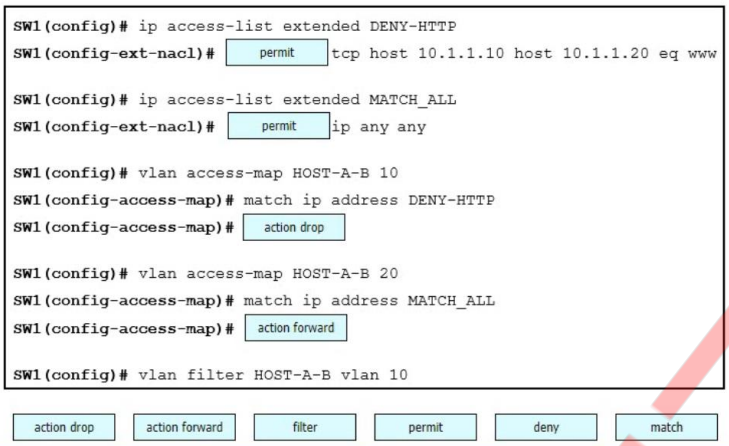
- ip sla 35
  icmp-echo 10.0.0.4 source-ip 10.0.100.3
  history buckets-kept 300
  ip sla schedule 35 life forever start-time now
- ip sla 35
  icmp-echo 10.0.100.3 source-ip 10.0.0.4
  frequency 300
  ip sla schedule 35 life forever start-time now
- ip sla 35
  icmp-echo 10.0.0.4 source-ip 10.0.100.3
  request-data-size 64
  ip sla schedule 35 life forever start-time now
- ip sla 35
  icmp-echo 10.0.0.1 source-ip 10.0.100.1
  timeout 300
  ip sla schedule 35 life forever start-time now

What is one fact about Cisco SD-Access wireless network deployments?

- The access point is part of the fabric overlay.
- The wireless client is part of the fabric overlay.
- The access point is part of the fabric underlay.
- The WLC is part of the fabric underlay.

+923342572268

Refer to the exhibit. An engineer must deny HTTP traffic from host A to host B while allowing all other communication between the hosts. Drag and drop the commands into the configuration to achieve these results. Some commands may be used more than once. Not all commands are used.



Which two mechanisms are available to secure NTP? (Choose two.)

- [ ] IP prefix list-based
- [ ] TACACS-based authentication
- [x] encrypted authentication
- [x] IP access list-based
- [ ] IPsec

+923342572268

```
#! /usr/bin/env python3

from env_lab import dnac
import json
import requests
import urllib3
from requests.auth import HTTPBasicAuth
from prettytable import PrettyTable

dnac_devices = PrettyTable(['Hostname','Platform Id','Software Type','Software Version','Up
Time' ])
dnac_devices.padding_width = 1
headers = {
        'content-type': "application/json",
        'x-auth-token': ""
      }

def dnac_login(host, username, password):
   url = "https://{}/api/system/v1/auth/token".format(host)
   response = requests.request("POST", url, auth=HTTPBasicAuth(username, password),
                       headers=headers, verify=False)
   return response.json()["Token"]

def network_device_list(dnac, token):
   url = "https://{}/api/v1/network-device".format(dnac['host'])
   headers["x-auth-token"] = token
   response = requests.get(url, headers=headers, verify=False)
   data = response.json()
   for item in data['response']:
      dnac_devices.add_row([item["hostname"],item["platformId"],item["softwareType"],item["soft
wareVersion"],item["upTime"]])
```

Refer to the exhibit. Which code results in the working Python script displaying a list of network devices from the Cisco DNA Center?

```
login = dnac_login(dnac["host"], dnac["username"], dnac["password"])

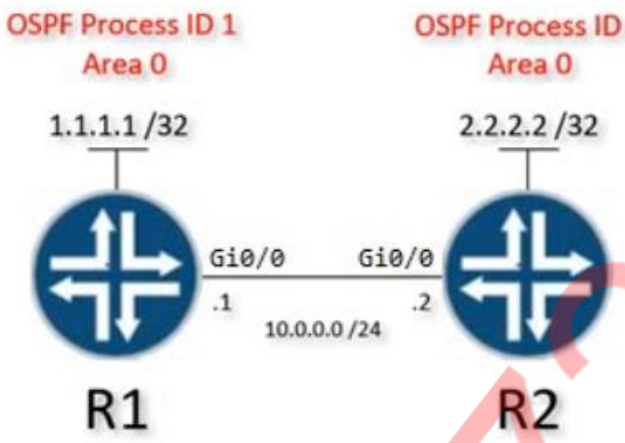
network_device_list(dnac, login)
for item in dnac_devices:
   print(dnac_devices.item)
```

```
login = dnac_login(dnac["host"], dnac["username"], dnac["password"])
network_device_list(dnac, login)
print(dnac_devices)
```

```
network_device_list(dnac["host"], dnac["username"],dnac["password"])
login = dnac_login(dnac)
print(dnac_devices)
```

```
network_device_list(dnac["host"], dnac["username"],dnac["password"])
login = dnac_login(dnac)
for item in dnac_devices:
   print(dnac_devices.item)
```

+923425722268



Router R1

```
router ospf 1
   router-id 1.1.1.1
   network 1.1.1.1 0.0.0.0 area 0
   network 10.0.0.0 0.0.0.255 area 0
```

Router R2

```
router ospf 1
   router-id 2.2.2.2
   network 2.2.2.2 0.0.0.0 area 0
   network 10.0.0.0 0.0.0.255 area 0
```

Refer to the exhibit. A network engineer is configuring OSPF between router R1 and router R2. The engineer must ensure that a DR/BDR election does not occur on the Gigabit Ethernet interfaces in area 0. Which configuration set accomplishes this goal?

- R1(config-if)**interface Gi0/0**
  R1(config-if)**ip ospf database-filter all out**

  R2(config-if)**interface Gi0/0**
  R2(config-if)**ip ospf database-filter all out**
- R1(config-if)**interface Gi0/0**
  R1(config-if)**ip ospf priority 1**

  R2(config-if)**interface Gi0/0**
  R2(config-if)**ip ospf priority 1**
- (selected) R1(config-if)**interface Gi0/0**
  R1(config-if)**ip ospf network point-to-point**

  R2(config-if)**interface Gi0/0**
  R2(config-if)**ip ospf network point-to-point**
- R1(config-if)**interface Gi0/0**
  R1(config-if)**ip ospf network broadcast**

  R2(config-if)**interface Gi0/0**
  R2(config-if)**ip ospf network broadcast**

What is provided by the Stealthwatch component of the Cisco Cyber Threat Defense solution?

- real-time threat management to stop DDoS attacks to the core and access networks
- (selected) real-time awareness of users, devices, and traffic on the network
- malware control
- dynamic threat control for web traffic

+923342572268

```
router ospf 43 vrf hotel
 router-id 3.3.3.3
 network 172.16.0.0 0.0.255.255 area 0

R1:
vrf definition bank
 !
 address-family ipv4
 exit-address-family
```

Refer to the exhibit. Which configuration must be applied to R1 to enable R1 to reach the server at 172.16.0.1?

- interface Ethernet0/0
  vrf forwarding bank
  ip address 172.16.0.7 255.255.0.0

  router ospf 44 vrf bank
  network 172.16.0.0 0.0.255.255 area 0

- interface Ethernet0/0
  ip address 172.16.0.7 255.255.0.0

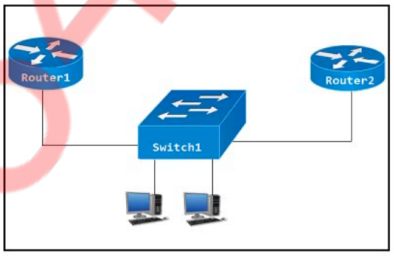
  router ospf 44 vrf bank
  network 172.16.0.0 255.255.0.0

- interface Ethernet0/0
  ip address 172.16.0.7 255.255.0.0

  router ospf 44 vrf hotel
  network 172.16.0.0 255.255.0.0

- interface Ethernet0/0
  vrf forwarding hotel
  ip address 172.16.0.7 255.255.0.0

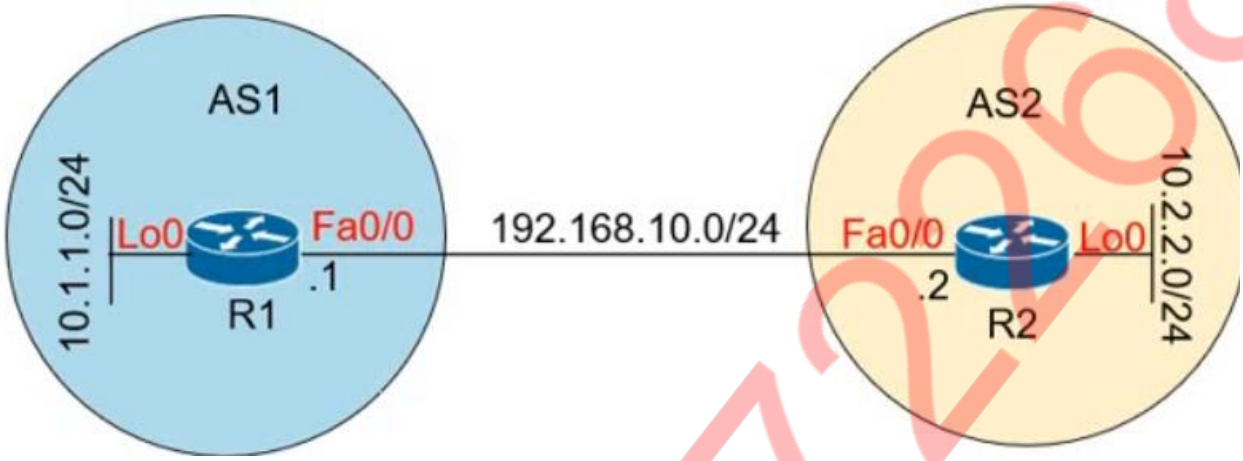
  router ospf 44 vrf Hotel
  network 172.16.0.0 0.0.255.255 area 0



Refer to the exhibit. Router1 is currently operating as the HSRP primary with a priority of 110. Router1 fails and Router2 takes over the forwarding role. Which command on Router1 causes it to take over the forwarding role when it returns to service?

- standby 2 priority
- standby 2 preempt
- standby 2 track
- standby 2 timers

+923342572268



Refer to the exhibit. Which configuration establishes EBGP neighborship between these two directly connected neighbors and exchanges the loopback network of the two routers through BGP?

- R1(config)#**router bgp 1**
  R1(config-router)#**neighbor 10.2.2.2 remote-as 2**
  R1(config-router)#**neighbor 10.2.2.2 update-source lo0**
  R1(config-router)#**network 10.1.1.0 mask 255.255.255.0**

  R2(config)#**router bgp 2**
  R2(config-router)#**neighbor 10.1.1.1 remote-as 1**
  R2(config-router)#**neighbor 10.1.1.1 update-source lo0**
  R2(config-router)#**network 10.2.2.0 mask 255.255.255.0**

- R1(config)#**router bgp 1**
  R1(config-router)#**neighbor 192.168.10.2 remote-as 2**
  R1(config-router)#**network 10.1.1.0 mask 255.255.255.0**

  R2(config)#**router bgp 2**
  R2(config-router)#**neighbor 192.168.10.1 remote-as 1**
  R2(config-router)#**network 10.2.2.0 mask 255.255.255.0**

- R1(config)#**router bgp 1**
  R1(config-router)#**neighbor 192.168.10.2 remote-as 2**
  R1(config-router)#**network 10.0.0.0 mask 255.0.0.0**

  R2(config)#**router bgp 2**
  R2(config-router)#**neighbor 192.168.10.1 remote-as 1**
  R2(config-router)#**network 10.0.0.0 mask 255.0.0.0**

- R1(config)#**router bgp 1**
  R1(config-router)#**neighbor 10.2.2.2 remote-as 2**
  R1(config-router)#**network 10.1.1.0 mask 255.255.255.0**

  R2(config)#**router bgp 2**
  R2(config-router)#**neighbor 10.1.1.1 remote-as 1**
  R2(config-router)#**network 10.2.2.0 mask 255.255.255.0**

Which command set configures RSPAN to capture outgoing traffic from VLAN 3 on interface GigabitEthernet 0/3 while ignoring other VLAN traffic on the same interface?

- **monitor session 2 source interface gigabitethernet0/3 tx**
  monitor session 2 filter vlan 1 - 2 , 4 - 4094

- **monitor session 2 source interface gigabitethernet0/3 rx**
  monitor session 2 filter vlan 3

- **monitor session 2 source interface gigabitethernet0/3 rx**
  monitor session 2 filter vlan 1 - 2 , 4 - 4094

- **monitor session 2 source interface gigabitethernet0/3 tx**
  monitor session 2 filter vlan 3

+923342572298

The login method is configured on the VTY lines of a router with these parameters:

- The first method for authentication is TACACS
- If TACACS is unavailable, login is allowed without any provided credentials

Which configuration accomplishes this task?

R1#**sh run | include aaa**
aaa new-model
aaa authentication login default group tacacs+ none
aaa session-id common

R1#**sh run | section vty**
line vty 0 4
password 7 02050D480809

R1#**sh run | include username**
R1#

R1#**sh run | include aaa**
aaa new-model
aaa authentication login default group tacacs+
aaa session-id common

R1#**sh run | section vty**
line vty 0 4
transport input none
R1#

R1#**sh run | include aaa**
aaa new-model
aaa authentication login telnet group tacacs+ none
aaa session-id common

R1#**sh run | section vty**
line vty 0 4

R1#**sh run | include username**
R1#

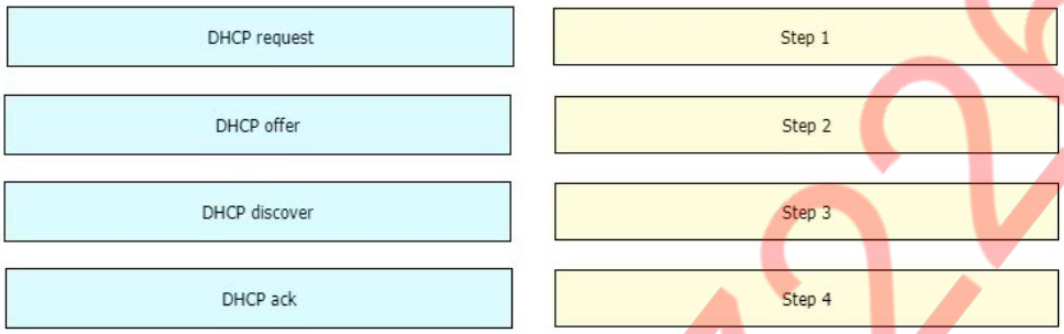
R1#**sh run | include aaa**
aaa new-model
aaa authentication login VTY group tacacs+ none
aaa session-id common

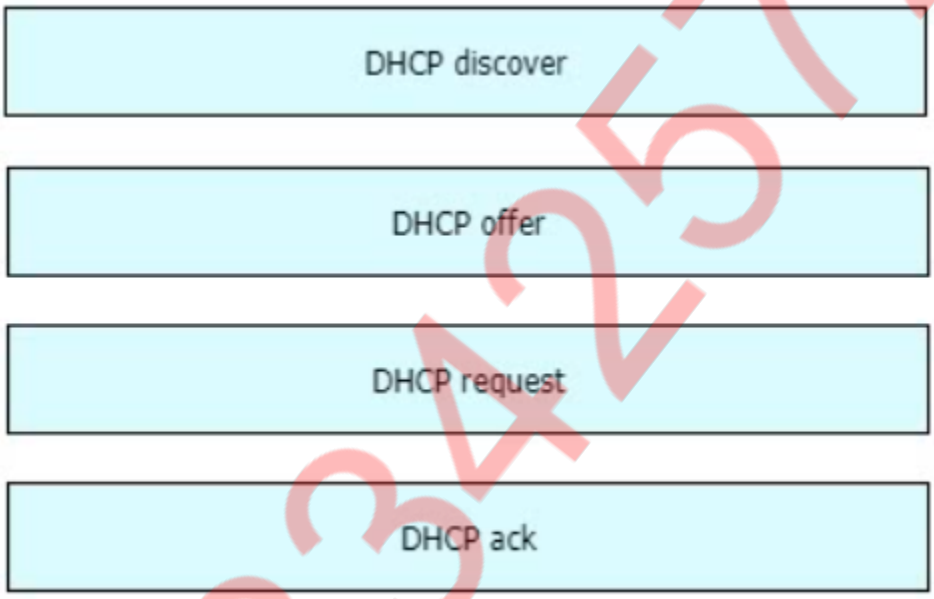
R1#**sh run | section vty**
line vty 0 4
password 7 02050D480809

R1#**sh run | include username**
R1#

+923342572268

Drag and drop the DHCP messages that are exchanged between a client and an AP into the order they are exchanged on the right.





+923342572268

```
Router#show ip ospf interface
GigabitEthernet0/1.40 is up, line protocol is up
  Internet Address 10.3.5.254/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 10.3.5.254
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 172.16.30.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 172.16.30.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 172.16.11.29/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 172.16.11.27, Interface address 172.16.11.27
  Backup Designated router (ID) 172.16.11.30, Interface address 172.16.11.30
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
```

Refer to the exhibit. A network engineer configures OSPF and reviews the router configuration. Which interface or interfaces are able to establish OSPF adjacency?

- only GigabitEthernet0/1
- GigabitEthernet0/0 and GigabitEthernet0/1
- only GigabitEthernet0/0
- GigabitEthernet0/1 and GigabitEthernet0/1.40

+923125172268

Name is Bob Johnson
Age is 75
Is alive

Favorite foods are:
• Cereal
• Mustard
• Onions

Refer to the exhibit. What is the JSON syntax that is formed from the data?

- {"Name": "Bob Johnson", "Age": Seventyfive, "Alive": true, "Favorite Foods": ["Cereal", "Mustard", "Onions"]}
- {"Name": "Bob Johnson", "Age": 75, "Alive": true, "Favorite Foods": ["Cereal", "Mustard", "Onions"]}
- {Name: Bob Johnson, Age: 75, Alive: true, Favorite Foods: [Cereal, Mustard, Onions]}
- {'Name': 'Bob Johnson', 'Age': 75, 'Alive': True, 'Favorite Foods': 'Cereal', 'Mustard', 'Onions'}

A network engineer is configuring Flexible NetFlow and enters these commands:

```
sampler NetFlow1
mode random one-out-of 100

interface fastethernet 1/0
flow-sampler NetFlow1
```

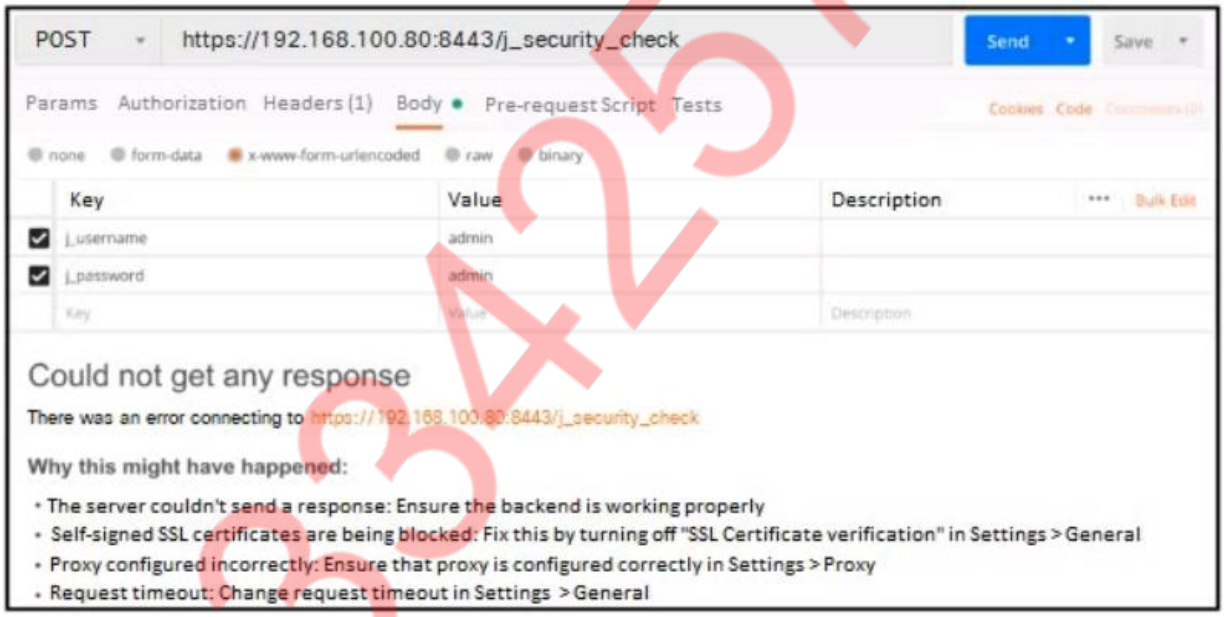
What are two results of implementing this feature instead of traditional NetFlow? (Choose two.)

- [ ] The accuracy of the data to be analyzed is improved.
- [x] The number of packets to be analyzed are reduced.
- [ ] Only the flows of top 100 talkers are exported.
- [x] CPU and memory utilization are reduced.
- [ ] The data export flow is more secure.

+923342572268

```
vedge-001# show control connections

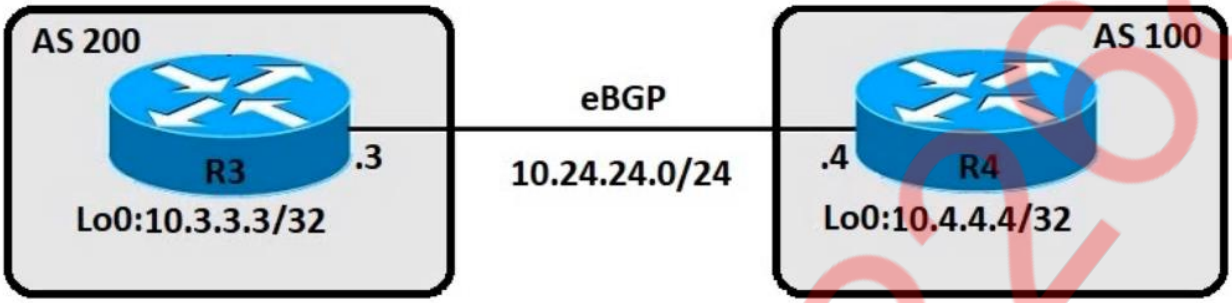
PEER                                          PEER
CONTROLLER
PEER    PEER PEER            SITE       DOMAIN PEER
PRIV  PEER                                 PUB
GROUP
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                                PORT
PUBLIC IP                                  PORT  LOCAL COLOR     PROXY STATE UPTIME      ID
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
------
vsmart  dtls 4.4.4.70        100        1      192.168.100.80
12446 10.10.20.70                                12446 default          No    up
0:02:24:09  0
vbond   dtls 0.0.0.0         0          0      192.168.100.81
12346 10.10.20.80                                12346 default          -     up
0:02:24:10  0
vmanage dtls 4.4.4.90        100        0      192.168.100.82
12446 10.10.20.90                                12446 default
```



Refer to the exhibit. What step resolves the authentication issue?

- use basic authentication
- change the port to 12446
- target 192.168.100.82 in the URI
- restart the vsmart host

+923342572268



Refer to the exhibit. An engineer must establish eBGP peering between router R3 and router R4. Both routers should use their loopback interfaces as the BGP router ID. Which configuration set accomplishes this task?

- R3(config)#**router bgp 200**
  R3(config-router)#**neighbor 10.4.4.4 remote-as 100**
  R3(config-router)#**neighbor 10.4.4.4 update-source Loopback0**

  R4(config)#**router bgp 100**
  R4(config-router)#**neighbor 10.3.3.3 remote-as 200**
  R4(config-router)#**neighbor 10.3.3.3 update-source Loopback0**

- R3(config)#**router bgp 200**
  R3(config-router)#**neighbor 10.4.4.4 remote-as 100**
  R3(config-router)#**bgp router-id 10.3.3.3**

  R4(config)#**router bgp 100**
  R4(config-router)#**neighbor 10.3.3.3 remote-as 200**
  R4(config-router)#**bgp router-id 10.4.4.4**

- R3(config)#**router bgp 200**
  R3(config-router)#**neighbor 10.24.24.4 remote-as 100**
  R3(config-router)#**bgp router-id 10.3.3.3**

  R4(config)#**router bgp 100**
  R4(config-router)#**neighbor 10.24.24.3 remote-as 200**
  R4(config-router)#**bgp router-id 10.4.4.4**

- R3(config)#**router bgp 200**
  R3(config-router)#**neighbor 10.24.24.4 remote-as 100**
  R3(config-router)#**neighbor 10.24.24.4 update-source Loopback0**

  R4(config)#**router bgp 100**
  R4(config-router)#**neighbor 10.24.24.3 remote-as 200**
  R4(config-router)#**neighbor 10.24.24.3 update-source Loopback0**

When a wireless client roams between two different wireless controllers, a network connectivity outage is experienced for a period of time. Which configuration issue would cause this problem?

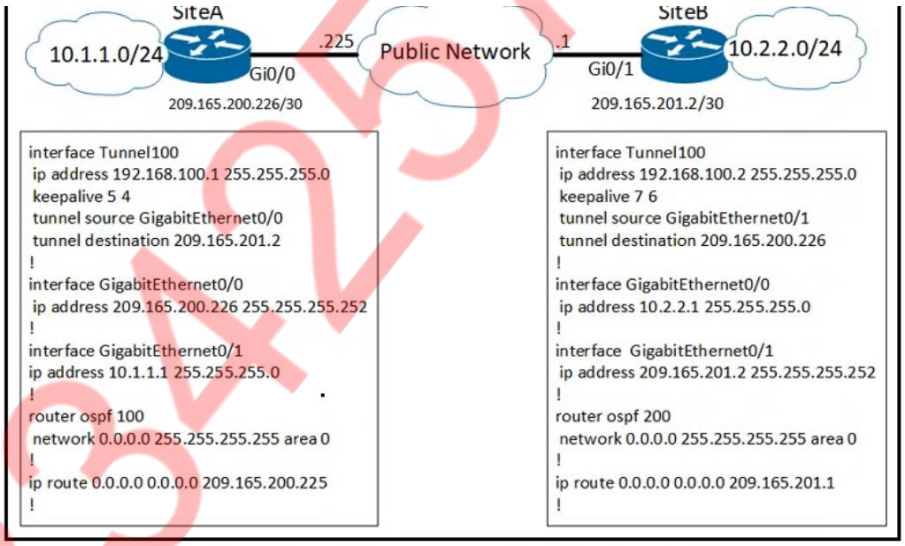
- Not all of the controllers in the mobility group are using the same mobility group name.
- Not all of the controllers within the mobility group are using the same virtual interface IP address.
- All of the controllers within the mobility group are using the same virtual interface IP address.
- All of the controllers in the mobility group are using the same mobility group name.

+923342572268

```
Extended IP access list EGRESS
10 permit ip 10.1.100.0 0.0.0.255 10.1.2.0 0.0.0.255
20 deny ip any any
```

Refer to the exhibit. An engineer must modify the access control list EGRESS to allow all IP traffic from subnet 10.1.10.0/24 to 10.1.2.0/24. The access control list is applied in the outbound direction on router interface GigabitEthernet 0/1. Which configuration command set will allow this traffic without disrupting existing traffic flows?

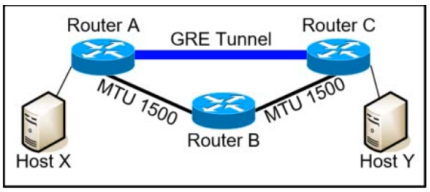
- config t
  ip access-list extended EGRESS
  permit ip 10.1.10.0 255.255.255.0 10.1.2.0 255.255.255.0
- **config t**
  ip access-list extended EGRESS
  5 permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
- config t
  ip access-list extended EGRESS
  permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
- config t
  ip access-list extended EGRESS2
  permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
  permit ip 10.1.100.0 0.0.0.255 10.1.2.0 0.0.0.255
  deny ip any any
  !
  interface g0/1
  no ip access-group EGRESS out
  ip access-group EGRESS2 out



Refer to the exhibit. A network engineer configures a new GRE tunnel and enters the **show run** command. What does the output verify?

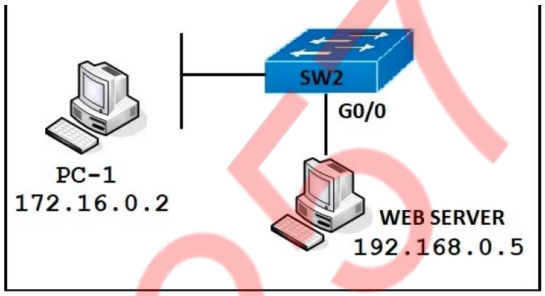
- The default MTU of the tunnel interface is 1500 bytes.
- The tunnel destination will be known via the tunnel interface.
- The tunnel will be established and work as expected.
- The tunnel keepalive is configured incorrectly because they must match on both sites.

+923342572268



Refer to the exhibit. MTU has been configured on the underlying physical topology, and no MTU command has been configured on the tunnel interfaces. What happens when a 1500-byte IPv4 packet traverses the GRE tunnel from host X to host Y, assuming the DF bit is cleared?

- The packet arrives on router C without fragmentation.
- The packet arrives on router C fragmented.
- The packet is discarded on router A.
- The packet is discarded on router B.



Refer to the exhibit. PC-1 must access the web server on port 8080. To allow this traffic, which statement must be added to an access control list that is applied on SW2 port G0/0 in the inbound direction?

- permit tcp host 192.168.0.5 host 172.16.0.2 eq 8080
- permit tcp host 192.168.0.5 eq 8080 host 172.16.0.2
- permit tcp host 192.168.0.5 lt 8080 host 172.16.0.2
- permit tcp host 172.16.0.2 host 192.168.0.5 eq 8080

How does the EIGRP metric differ from the OSPF metric?

- The EIGRP metric is calculated based on bandwidth only. The OSPF metric is calculated on delay only.
- The EIGRP metric is calculated based on delay only. The OSPF metric is calculated on bandwidth and delay.
- The EIGRP metric is calculated based on bandwidth and delay. The OSPF metric is calculated on bandwidth only.
- The EIGRP metric is calculated based on hop count and bandwidth. The OSPF metric is calculated on bandwidth and delay.

What is a VPN in a Cisco SD-WAN deployment?

- common exchange point between two different services
- attribute to identify a set of services offered in specific places in the SD-WAN fabric
- virtualized environment that provides traffic isolation and segmentation in the SD-WAN fabric
- virtual channel used to carry control plane information

+923342572268

An engineer is concerned with the deployment of a new application that is sensitive to inter-packet delay variance. Which command configures the router to be the destination of jitter measurements?

- Router(config)# **ip sla responder tcp-echo 172.29.139.134 5000**
- Router(config)# **ip sla responder udp-connect 172.29.139.134 5000**
- Router(config)# **ip sla responder tcp-connect 172.29.139.134 5000**
- Router(config)# **ip sla responder udp-echo 172.29.139.134 5000**

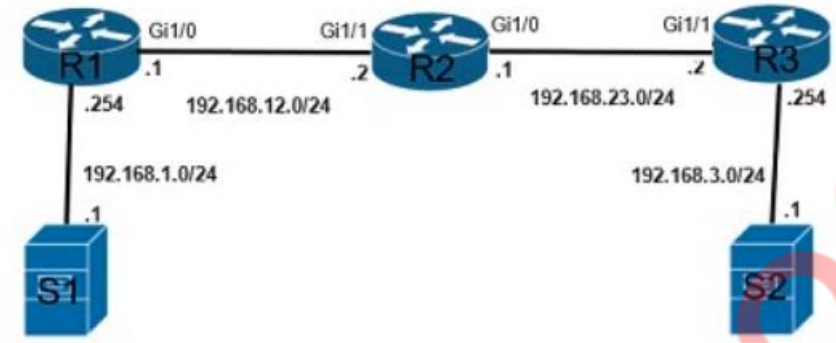
Which AP mode allows a supported AP to function like a WLAN client would, associating and identifying client connectivity issues?

- client mode
- SE-connect mode
- sensor mode
- sniffer mode

Which technology does VXLAN use to provide segmentation for Layer 2 and Layer 3 traffic?

- VRF
- VLAN
- VNI
- bridge domain

+923342572268




```
Frame 7: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
Ethernet II, Src: Vmware_8e:02:44 (00:50:56:8e:02:44), Dst: CiscoInc_8b:36:d1 (00:1d:a1:8b:36:d1)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.3.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 92
  Identification: 0x03c7 (967)
> Flags: 0x00
  Fragment offset: 0
> Time to live: 2
  Protocol: ICMP (1)
> Header checksum: 0x0000 [validation disabled]
  Source: 192.168.1.1
  Destination: 192.168.3.1
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf783 [correct]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 123 (0x007b)
  Sequence number (LE): 31488 (0x7b00)
> [No response seen]
> Data (64 bytes)
```

Refer to the exhibit. While troubleshooting a routing issue, an engineer issues a ping from S1 to S2. Which two actions result from the initial value of the TTL? (Choose two.)

- [x] The packet reaches R3, and the TTL expires.
- [x] R3 replies with a TTL exceeded message.
- [ ] R1 replies with a TTL exceeded message.
- [ ] The packet reaches R2, and the TTL expires.
- [ ] The packet reaches R1, and the TTL expires.
- [ ] R2 replies with a TTL exceeded message.

+923425712268

Which configuration restricts the amount of SSH traffic that a router accepts to 100 kbps?

```
class-map match-all CoPP_SSH
      match access-group name CoPP_SSH
      !
policy-map CoPP_SSH
      class CoPP_SSH
   police cir 100000
      exceed-action drop
      !
!
!
   interface GigabitEthernet0/1
      ip address 209.165.200.225 255.255.255.0
      ip access-group EGRESS out
      service-policy input CoPP_SSH
!
    ip access-list extended CoPP_SSH
       permit tcp any any eq 22
```

```
class-map match-all CoPP_SSH
      match access-group name CoPP_SSH
      !
policy-map CoPP_SSH
      class CoPP_SSH
   police cir 100000
      exceed-action drop
      !
!
!
   interface GigabitEthernet0/1
      ip address 209.165.200.225 255.255.255.0
      ip access-group EGRESS out
      service-policy input CoPP_SSH
!
   ip access-list extended CoPP_SSH
```

```
class-map match-all CoPP_SSH
      match access-group name CoPP_SSH
      !
policy-map CoPP_SSH
      class CoPP_SSH
   police cir 100000
      exceed-action drop
      !
!
!
   control-plane
      service-policy input CoPP_SSH
!
   ip access-list extended CoPP_SSH
      permit tcp any any eq 22
```

```
class-map match-all CoPP_SSH
      match access-group name CoPP_SSH
      !
policy-map CoPP_SSH
      class CoPP_SSH
   police cir 100000
      exceed-action drop
      !
!
!
   control-plane transit
      service-policy input CoPP_SSH
!
   ip access-list extended CoPP_SSH
      permit tcp any any eq 22
```

+923342572268

Which method creates an EEM applet policy that is registered with EEM and runs on demand or manually?

- **event manager applet ondemand**
  event register
  action 1.0 syslog priority critical msg 'This is a message from ondemand'
- **event manager applet ondemand**
  event none
  action 1.0 syslog priority critical msg 'This is a message from ondemand'
- **event manager applet ondemand**
  event manual
  action 1.0 syslog priority critical msg 'This is a message from ondemand'
- **event manager applet ondemand**
  action 1.0 syslog priority critical msg 'This is a message from ondemand'

Wireless users report frequent disconnections from the wireless network. While troubleshooting, a network engineer finds that after the user is disconnected, the connection re-establishes automatically without any input required. The engineer also notices these message logs:

AP 'AP2' is down. Reason: Radio channel set. 6:54:04 PM
AP 'AP4' is down. Reason: Radio channel set. 6:44:49 PM
AP 'AP7' is down. Reason: Radio channel set. 6:34:32 PM

Which action reduces the user impact?

- enable BandSelect
- enable coverage hole detection
- increase the dynamic channel assignment interval
- increase the AP heartbeat timeout

Which new enhancement was implemented in Wi-Fi 6?

- 4096 Quadrature Amplitude Modulation Mode
- Channel bonding
- Wi-Fi Protected Access 3
- Uplink and Downlink Orthogonal Frequency Division Multiple Access

+923342572268

When configuring WPA2 Enterprise on a WLAN, which additional security component configuration is required?

- (•) RADIUS server
- ( ) TACACS server
- ( ) PKI server
- ( ) NTP server

Which statement about TLS is accurate when using RESTCONF to write configurations on network devices?

- ( ) It is not supported on Cisco devices.
- ( ) It is used for HTTP and HTTPS requests.
- (•) It is provided using NGINX acting as a proxy web server.
- ( ) It requires certificates for authentication.

```
ip nat pool Internet 10.10.10.1 10.10.10.100 netmask 255.255.255.0
ip nat inside source route-map Users pool Internet
!
ip access-list standard Users
 10 permit 192.168.1.0 0.0.0.255
!
route-map Users permit 10
 match ip address Users
```

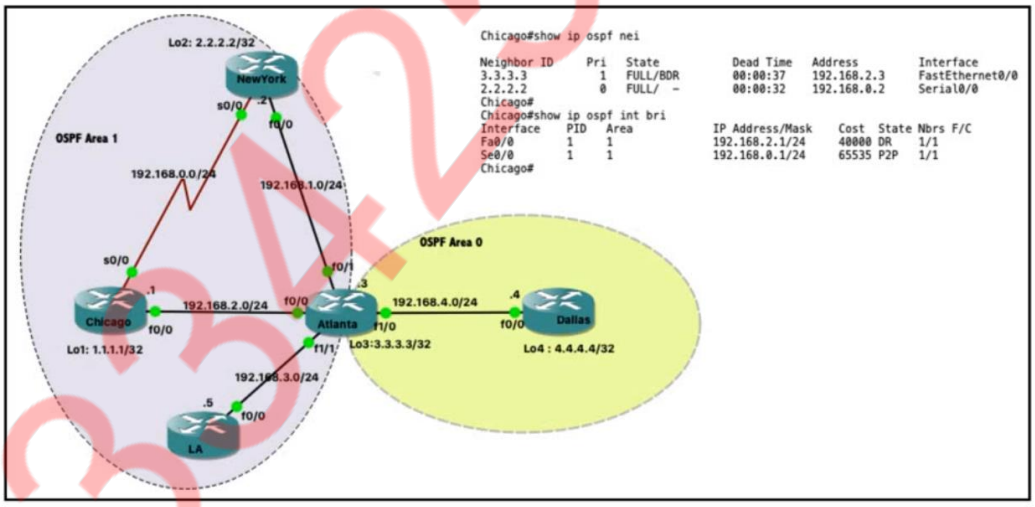
Refer to the exhibit. Which action completes the configuration to achieve a dynamic continuous mapped NAT for all users?

- ( ) Reconfigure the pool to use the 192.168.1.0 address range.
- (•) Increase the NAT pool size to support 254 usable addresses.
- ( ) Configure a match-host type NAT pool.
- ( ) Configure a one-to-one type NAT pool.

+923425722268

What is a characteristic of a next-generation firewall?

- only required at the network perimeter
- required in each layer of the network
- filters traffic using Layer 3 and Layer 4 information only
- provides intrusion prevention

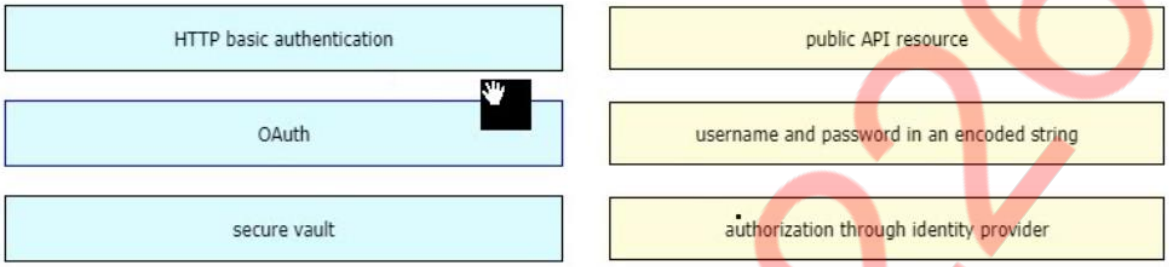


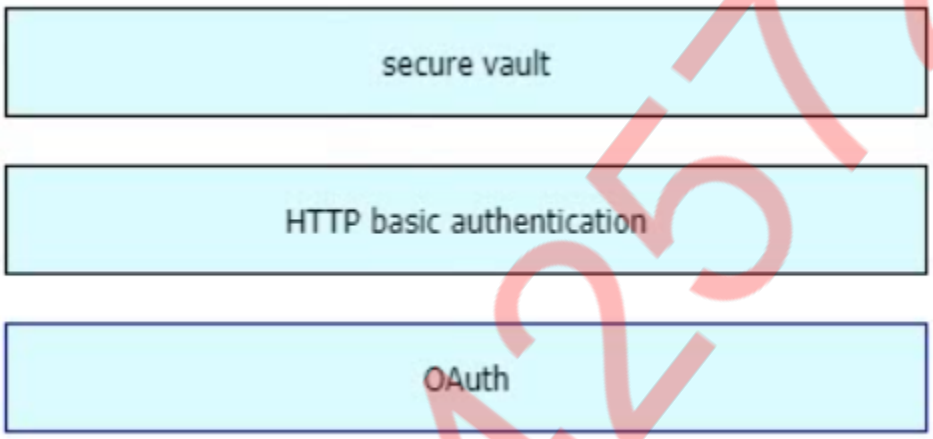
Refer to the exhibit. Which router is the designated router on the segment 192.168.0.0/24?

- This segment has no designated router because it is a nonbroadcast network type.
- This segment has no designated router because it is a p2p network type.
- Router NewYork because it has a higher router ID.
- Router Chicago because it has a lower router ID.

+923425722268

Drag and drop the REST API authentication methods from the left onto their descriptions on the right.



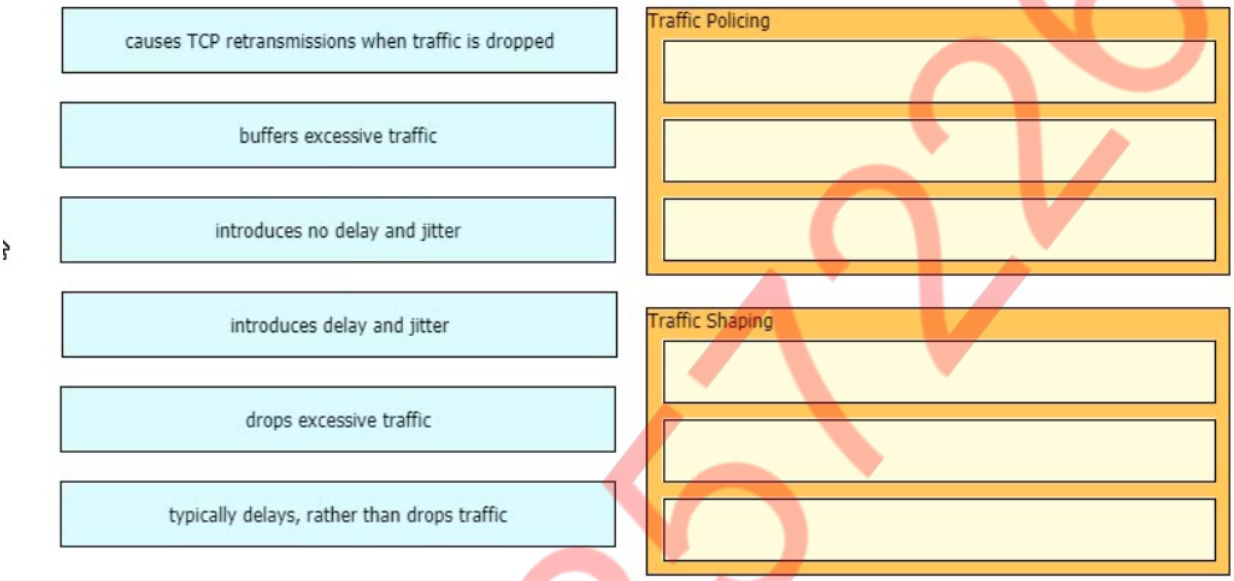


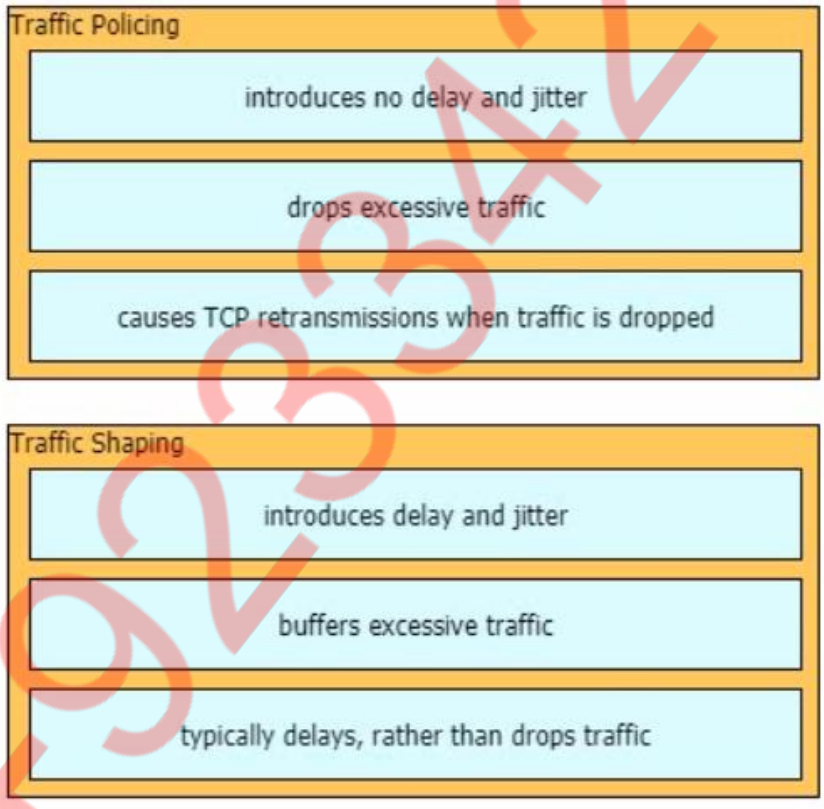
Which function does a fabric edge node perform in a Cisco SD-Access deployment?

- encapsulates end-user data traffic into LISP
- provides reachability between border nodes in the fabric underlay
- connects the SD-Access fabric to another fabric or external Layer 3 networks
- connects endpoints to the fabric and forwards their traffic

+923342572268

Drag and drop the descriptions from the left onto the QoS components on the right.





+923342567268

What is the function of the fabric control plane node in a Cisco SD-Access deployment?

- It is responsible for policy application and network segmentation in the fabric.
- It performs traffic encapsulation and security profiles enforcement in the fabric.
- (•) It holds a comprehensive database that tracks endpoints and networks in the fabric.
- It provides integration with legacy nonfabric-enabled environments.

What is the difference between a RIB and a FIB?

- The RIB is used to make IP source prefix-based switching decisions.
- (•) The FIB is populated based on RIB content.
- The RIB maintains a mirror image of the FIB.
- The FIB is where all IP routing information is stored.

What is a benefit of data modeling languages like YANG?

- They create more secure and efficient SNMP OIDs.
- (•) They provide a standardized data structure, which results in configuration scalability and consistency.
- They enable programmers to change or write their own applications within the device operating system.
- They make the CLI simpler and more efficient.

+923342572268

Which method does Cisco DNA Center use to allow management of non-Cisco devices through southbound protocols?

- (•) It creates device packs through the use of an SDK.
- ( ) It uses an API call to interrogate the devices and register the returned data.
- ( ) It obtains MIBs from each vendor that details the APIs available.
- ( ) It imports available APIs for the non-Cisco device in a CSV format.

Which entity is responsible for maintaining Layer 2 isolation between segments in a VXLAN environment?

- ( ) VTEP
- ( ) host switch
- ( ) switch fabric
- (•) VNID

What do Cisco DNA southbound APIs provide?

- ( ) interface between the controller and the consumer
- ( ) RESTful API interface for orchestrator communication
- (•) interface between the controller and the network devices
- ( ) NETCONF API interface for orchestrator communication

+923342572268

What is required for a virtual machine to run?

- (•) a Type 1 hypervisor and a host operating system
- ( ) a hypervisor and physical server hardware
- ( ) only a Type 1 hypervisor
- ( ) only a Type 2 hypervisor

Which two GRE features are configured to prevent fragmentation? (Choose two.)

- [x] IP MTU
- [ ] TCP window size
- [x] TCP MSS
- [ ] MTU ignore
- [ ] DF bit clear

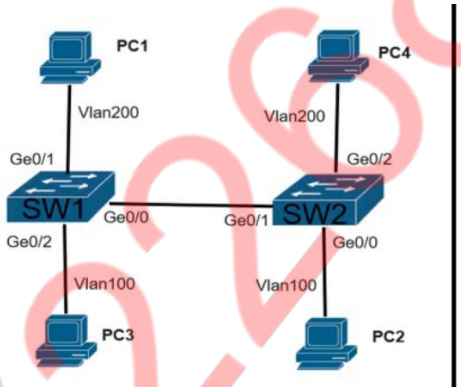
Which benefit is offered by a cloud infrastructure deployment but is lacking in an on-premises deployment?

- ( ) supported systems
- ( ) storage capacity
- (•) efficient scalability
- ( ) virtualization

+923342572268

```
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (NATIVE)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
...output omitted...

SW2# show interfaces gigabitethernet 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (NATIVE)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
...output omitted...
```



Refer to the exhibit. The connection between SW1 and SW2 is not operational. Which two actions resolve the issue? (Choose two.)

- [ ] configure **switchport nonegotiate** on SW1
- [x] configure **switchport mode trunk** on SW2
- [x] configure **switchport mode dynamic desirable** on SW2
- [ ] configure **switchport nonegotiate** on SW2
- [ ] configure **switchport mode access** on SW2

What does the LAP send when multiple WLCs respond to the CISCO-CAPWAP-CONTROLLER.localdomain hostname during the CAPWAP discovery and join process?

- ( ) multicast discovery request
- ( ) unicast discovery request to the first WLC that resolves the domain name
- (•) join request to all the WLCs
- ( ) unicast discovery request to each WLC

Which outcome is achieved with this Python code?

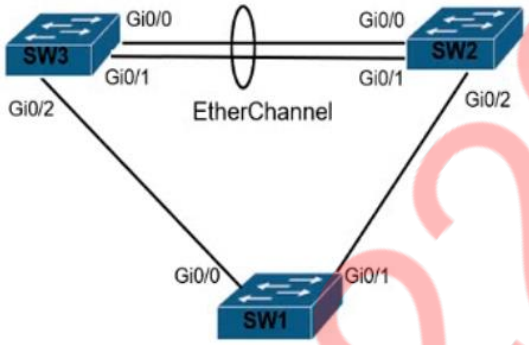
```
client.connect ( ip,  port= 22, username= usr, password= pswd )
stdin,  stdout, stderr = client.exec_command ( 'show ip bgp 192.168.101.0 bestpath\n ' )
print (stdout)
```

- (•) connects to a Cisco device using SSH and exports the BGP table for the prefix
- ( ) displays the output of the **show** command in a formatted way
- ( ) connects to a Cisco device using Telnet and exports the routing table information
- ( ) connects to a Cisco device using SSH and exports the routing table information

+923342572268

```
SW2# show etherchannel summary
Flags: D - down P - bundled in
port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate
aggregator
M - not in use, minimum links not
met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+-------------+-----------+--
-----------------------------------
-
1 Po1(S D ) LACP Gi0/0(I) Gi0/1(I)

SW3# show etherchannel summary
Flags: D - down P - bundled in
port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP onl
R - Layer3 S - Layer2
U - in use f - failed to allocate
aggregator
M - not in use, minimum links not
met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+-------------+-----------+--
-----------------------------------
-
1 Po1(S D ) LACP Gi0/0(I) Gi0/1(I)
```




```
SW2# show run interface
gigabitethernet 0/0
Building configuration...
Current configuration : 189 bytes
!
interface GigabitEthernet0/0
switchport trunk encapsulation isl
switchport mode access
switchport nonegotiate
channel-group 1 mode active
end

SW3# show run interface
gigabitethernet 0/0
Building configuration...
Current configuration : 151 bytes
!
interface GigabitEthernet0/0
switchport trunk encapsulation isl
switchport mode trunk
switchport nonegotiate
channel-group 1 mode passive
end
```

```
SW2# show run interface
gigabitethernet 0/1
Building configuration...
Current configuration : 189 bytes
!
interface GigabitEthernet0/1
switchport trunk encapsulation isl
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active
end

SW3# show run interface
gigabitethernet 0/1
Building configuration...
Current configuration : 151 bytes
!
interface GigabitEthernet0/1
switchport trunk encapsulation isl
switchport mode trunk
switchport nonegotiate
channel-group 1 mode passive
end
```

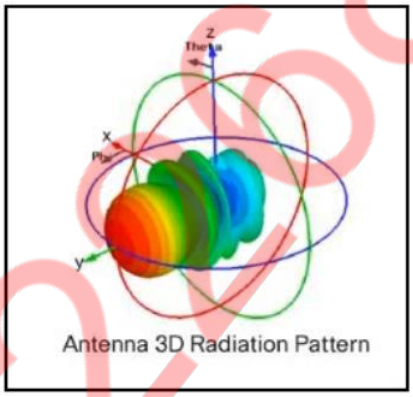
Refer to the exhibit. The EtherChannel between SW2 and SW3 is not operational. Which action resolves this issue?

- Configure the mode on SW2 Gi0/1 to access.
- Configure the channel-group mode on SW3 Gi0/0 and Gi0/1 to active.
- Configure the mode on SW2 Gi0/0 to trunk.
- Configure the channel-group mode on SW2 Gi0/0 and Gi0/1 to on.

Which characteristic distinguishes Ansible from Chef?

- The Ansible server can run on Linux, Unix or Windows. The Chef server must run on Linux or Unix.
- Ansible uses Ruby to manage configurations. Chef uses YAML to manage configurations.
- Ansible lacks redundancy support for the primary server. Chef runs two primary servers in active/active mode.
- Ansible pushes the configuration to the client. Chef client pulls the configuration from the server.

+923345757268



Refer to the exhibit. Which type of antenna does the radiation pattern represent?

- omnidirectional
- Yagi
- multidirectional
- directional patch

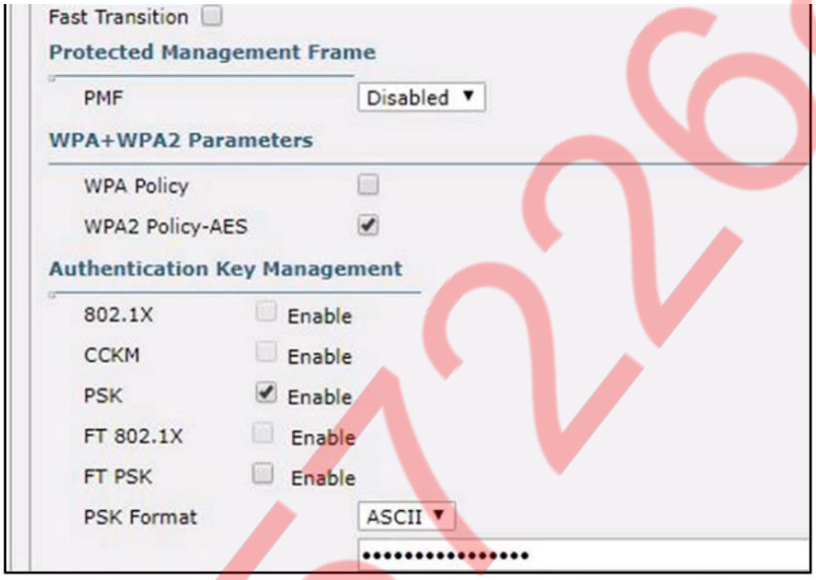
What is a characteristic of YANG?

- It is a Cisco proprietary language that models NETCONF data.
- It allows model developers to create custom data types.
- It structures data in an object-oriented fashion to promote model reuse.
- It provides loops and conditionals to control flow within models.

Which HTTP status code is the correct response for a request with an incorrect password applied to a REST API session?

- HTTP Status Code: 200
- HTTP Status Code: 302
- HTTP Status Code: 401
- HTTP Status Code: 504

+923342572568



Refer to the exhibit. Based on the configuration in this WLAN security setting, which method can a client use to authenticate to the network?

- RADIUS token
- certificate
- text string
- username and password

What is the function of a fabric border node in a Cisco SD-Access environment?

- To collect traffic flow information toward external networks.
- To connect the Cisco SD-Access fabric to another fabric or external Layer 3 networks.
- To attach and register clients to the fabric.
- To handle an ordered list of IP addresses and locations for endpoints in the fabric.

Under which network conditions is an outbound QoS policy that is applied on a router WAN interface most beneficial?

- under network convergence conditions
- under interface saturation conditions
- under all network conditions
- under traffic classification and marking conditions

+923342572268

A network administrator has designed a network with two multilayer switches on the distribution layer, which act as default gateways for the end hosts. Which two technologies allow every end host in a VLAN to use both gateways? (Choose two.)

- [x] GLBP
- [ ] HSRP
- [ ] VSS
- [ ] VRRP
- [x] MHSRP

```
SW1#sh monitor session all
Session 1
------------
Type                   : Remote Destination Session
Source RSPAN VLAN      : 50

Session 2
------------
Type                   : Local Session
Source Ports           :
    Both               : Fa0/14
  Destination Ports    : Fa0/15
    Encapsulation      : Native
          Ingress      : Disables
```

Refer to the exhibit. An engineer configures monitoring on SW1 and enters the **show** command to verify operation. What does the output confirm?

- (•) RSPAN session 1 is incompletely configured for monitoring.
- ( ) SPAN session 2 only monitors egress traffic exiting port FastEthernet 0/14.
- ( ) SPAN session 2 monitors all traffic entering and exiting port FastEthernet 0/15.
- ( ) RSPAN session 1 monitors activity on VLAN 50 of a remote switch.

What is the structure of a JSON web token?

- (•) three parts separated by dots: header, payload, and signature
- ( ) three parts separated by dots: version, header, and signature
- ( ) payload and signature
- ( ) header and payload

+923342572268

Which two components are supported by LISP? (Choose two.)

- [x] proxy ETR
- [x] egress tunnel router
- [ ] route reflector
- [ ] HMAC algorithm
- [ ] spoke

Which device makes the decision for a wireless client to roam?

- (•) wireless client
- ( ) wireless LAN controller
- ( ) access point
- ( ) WCS location server

How does EIGRP differ from OSPF?

- (•) EIGRP supports equal or unequal path cost, and OSPF supports only equal path cost.
- ( ) EIGRP is more prone to routing loops than OSPF.
- ( ) EIGRP has a full map of the topology, and OSPF only knows directly connected neighbors.
- ( ) EIGRP uses more CPU and memory than OSPF.

+923342572268

```
with manager.connect(host=192.168.0.1, port=22,
                     username='admin', password='password1', hostkey_verify=True,
                     device_params={'name':'nexus'}) as m:
```

Refer to the exhibit. What does the snippet of code achieve?

- It opens a tunnel and encapsulates the login information, if the host key is correct.
- It opens an ncclient connection to a Cisco Nexus device and maintains it for the duration of the context.
- It creates an SSH connection using the SSH key that is stored, and the password is ignored.
- It creates a temporary connection to a Cisco Nexus device and retrieves a token to be used for API calls.

Which three methods does Cisco DNA Center use to discover devices? (Choose three.)

- [x] CDP
- [ ] SNMP
- [x] LLDP
- [ ] ping
- [ ] NETCONF
- [x] a specified range of IP addresses

What are two benefits of virtual switching when compared to hardware switching? (Choose two.)

- [x] increased flexibility
- [x] VM-level isolation
- [ ] increased MTU size
- [ ] extended 802.1Q VLAN range
- [ ] hardware independence

+923342572268

An engineer has deployed a single Cisco 5520 WLC with a management IP address of 172.16.50.5/24. The engineer must register 50 new Cisco AIR-CAP2802I-E-K9 access points to the WLC using DHCP option 43. The access points are connected to a switch in VLAN 100 that uses the 172.16.100.0/24 subnet. The engineer has configured the DHCP scope on the switch as follows:

Network 172.16.100.0 255.255.255.0
Default Router 172.16.100.1
Option 43 ASCII 172.16.50.5

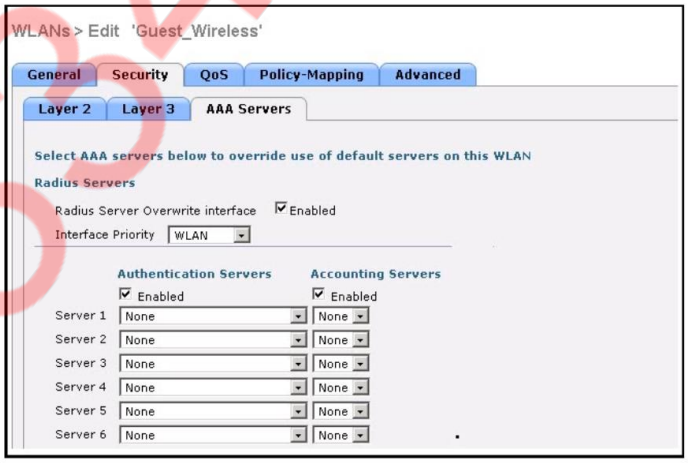
The access points are failing to join the wireless LAN controller. Which action resolves the issue?

- configure **option 43 Hex F104.AC10.3205**
- configure **option 43 Hex F104.CA10.3205**
- configure **dns-server 172.16.50.5**
- configure **dns-server 172.16.100.1**

```
%OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.2 on FastEthernet0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
%OSPF-6-AREACHG: 10.0.0.1/32 changed from area 0 to area 1
%OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from
backbone area must be virtual-link but not found from 10.0.0.2,
FastEthernet0/0
```

Refer to the exhibit. What is the cause of the log messages?

- OSPF area change
- IP address mismatch
- hello packet mismatch
- MTU mismatch



Refer to the exhibit. Assuming the WLC's interfaces are not in the same subnet as the RADIUS server, which interface would the WLC use as the source for all RADIUS-related traffic?

- the controller virtual interface
- the controller management interface
- any interface configured on the WLC
- the interface specified on the WLAN configuration

+923334251268

A customer has several small branches and wants to deploy a Wi-Fi solution with local management using CAPWAP. Which deployment model meets this requirement?

- SD-Access wireless
- Mobility Express
- local mode
- autonomous

Which data is properly formatted with JSON?

```
{
        "name": "Peter",
        "age": "25",
        "likesJson": true,
        "characteristics": ["small","strong","18"],
}
```

```
{
        "name":  Peter,
        "age": 25,
        "likesJson": true,
        "characteristics": ["small","strong","18"],
}
```

```
{
        "name": "Peter",
        "age": "25",
        "likesJson": true,
        "characteristics": ["small","strong",18]
}
```

```
{
        "name":"Peter"
        "age":"25"
        "likesJson":true
        "characteristics":["small","strong",18]
}
```

+923425722268

```
DSW2#sh spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    4106
             Address     0018.7363.4300
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4106  (priority 4096 sys-id-ext 20)
             Address     0018.7363.4300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa1/0/7             Desg FWD 2         128.9    P2p Peer(STP)
Fa1/0/10            Desg FWD 4         128.12   P2p Peer(STP)
Fa1/0/11            Desg FWD 2         128.13   P2p Peer(STP)
Fa1/0/12            Desg FWD 2         128.14   P2p Peer(STP)
```

Refer to the exhibit. What is the result when a switch that is running PVST+ is added to this network?

- Both switches operate in the PVST+ mode.
- Both switches operate in the Rapid PVST+ mode.
- Spanning tree is disabled automatically on the network.
- DSW2 operates in Rapid PVST+ and the new switch operates in PVST+.

```
Router#sh run | b vty
line vty 0 4
 session-timeout 30
 exec-timeout 120 0
 session-limit 30
 login local
line vty 5 15
 session-timeout 30
 exec-timeout 30 0
 session-limit 30
 login local
```

Refer to the exhibit. Security policy requires all idle exec sessions to be terminated in 600 seconds. Which configuration achieves this goal?

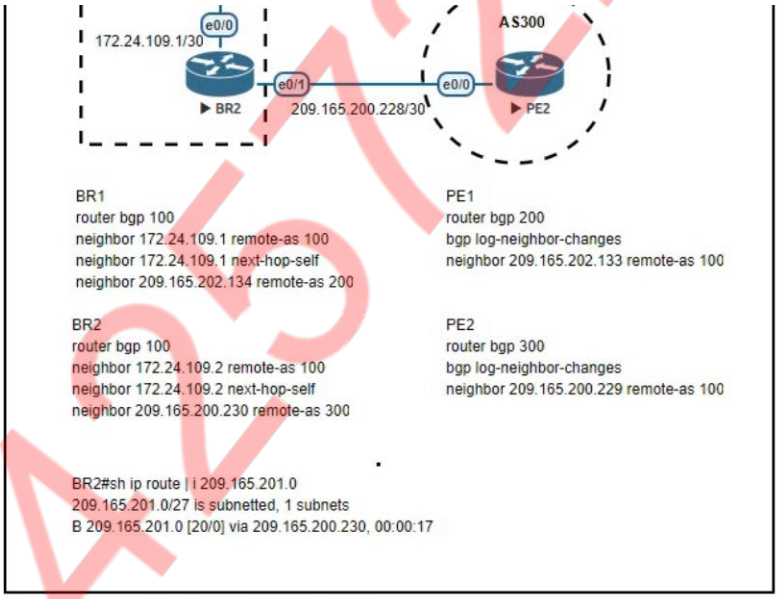
- **line vty 0 15**
  exec-timeout 10 0
- **line vty 0 15**
  absolute-timeout 600
- **line vty 0 4**
  exec-timeout 600
- **line vty 0 15**
  no exec-timeout

+923342572268

An engineer must create an EEM applet that sends a syslog message in the event a change happens in the network due to trouble with an OSPF process. Which action should the engineer use?

```
event manager applet LogMessage
  event routing network 172.30.197.0/24 type all
```

- action 1 syslog msg "OSPF ROUTING ERROR"
- action 1 syslog send "OSPF ROUTING ERROR"
- action 1 syslog pattern "OSPF ROUTING ERROR"
- action 1syslog write "OSPF ROUTING ERROR"



Refer to the exhibit. Which configuration change will force BR2 to reach 209.165.201.0/27 via BR1?

- Set the weight attribute to 65,535 on BR1 toward PE1.
- Set the MED to 1 on PE2 toward BR2 outbound.
- Set the origin to igp on BR2 toward PE2 inbound.
- Set the local preference to 150 on PE1 toward BR1 outbound.

In a three-tier hierarchical campus network design, which action is a design best-practice for the core layer?

- provide QoS prioritization services such as marking, queueing, and classification for critical network traffic
- provide redundant Layer 3 point-to-point links between the core devices for more predictable and faster convergence
- provide advanced network security features such as 802.1X, DHCP snooping, VACLs, and port security
- provide redundant aggregation for access layer devices and first-hop redundancy protocols such as VRRP

+923342572268

Which entity is a Type 1 hypervisor?

- Oracle VM VirtualBox
- VMware server
- Citrix XenServer
- Microsoft Virtual PC

How do cloud deployments differ from on-premises deployments?

- Cloud deployments require less frequent upgrades than on-premises deployments
- Cloud deployments require longer implementation times than on-premises deployments.
- Cloud deployments have lower upfront costs than on-premises deployments.
- Cloud deployments are more customizable than on-premises deployments.

Which outbound access list, applied to the WAN interface of a router, permits all traffic except for http traffic sourced from the workstation with IP address 10.10.10.1?

- ip access-list extended 100
  deny tcp host 10.10.10.1 any eq 80
  permit ip any any
- ip access-list extended 10
  deny tcp host 10.10.10.1 any eq 80
  permit ip any any
- ip access-list extended 200
  deny tcp host 10.10.10.1 eq 80 any
  permit ip any any
- ip access-list extended NO_HTTP
  deny tcp host 10.10.10.1 any eq 80

+923342572268